

IMPLEMENTASI WEB VULNERABILITY SCANNER
SEBAGAI ADD ONS GOOGLE CHROME

SKRIPSI



Oleh :

ADITYA WARDANA
0734010035

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”
JAWA TIMUR
2011

IMPLEMENTASI WEB VULNERABILITY SCANNER
SEBAGAI ADD ONS GOOGLE CHROME

SKRIPSI

Diajukan Untuk Memenuhi Sebagian Persyaratan
Dalam Memperoleh Gelar Sarjana Komputer
Jurusan Teknik Informatika



Oleh :

ADITYA WARDANA
0734010035

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2011

ABSTRAKSI

Aditya Wardana, 2001. Implementasi Web Vulnerability Scanner sebagai Add Ons Google Chrome (dibimbing oleh Basuki Rahmat, S.Si., MT dan Achmad Junaidi, S.Kom)

Internet pada era ini, sudah merebak di masyarakat. Namun para pengguna internet belum memperhatikan segi keamanannya, khususnya mengenai SQL Injection dan XSS Injection. Maka perlu dikembangkan aplikasi Web Vulnerability Scanner sebagai Add Ons Google Chrome dengan pola pendeteksian yang baik. Sehingga website yang masih mempunyai kelemahan terhadap SQL Injection dan XSS Injection dapat segera diperbaiki.

Dalam Skripsi ini, aplikasi dirancang dengan bahasa pemrograman JavaScript. Aplikasi ini mencari perbedaan antara sebelum dengan sesudah dimodifikasi alamat Url yang dikirim ke web server untuk mengetahui adanya pola yang menunjukkan adanya kelemahan terhadap SQL Injection dan XSS Injection. Aplikasi bisa melakukan scanning secara Online dan Offline. Hasil scanning ditampilkan langsung oleh aplikasi dan bisa disimpan secara permanen dalam bentuk file dokumen untuk dipergunakan guna memperbaiki website tersebut suatu saat nanti.

Dilakukan ujicoba terhadap aplikasi ini dengan 10 website. Dari 10 website yang diacak untuk dites dan ditemukan rata-rata nilai yaitu 5 dari 10 website terindikasi mengandung SQL Injection dengan nilai 23.6% terdikasi positif SQL Injection dari keseluruhan alamat Url, sedangkan yang terindikasi mengandung XSS Injection terdapat 7 dari 10 website dengan nilai 17.1% terindikasi positif XSS Injection dari keseluruhan alamat Url.

Kata kunci: Web Vulnerability Scanner, XSS Injection dan SQL Injection.

KATA PENGANTAR

Alhamdulillah, dengan mengucapkan puji dan syukur kehadiran Allah SWT atas rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul “IMPLEMENTASI WEB VULNERABILITY SCANNER SEBAGAI ADD ONS GOOGLE CHROME” yang merupakan persyaratan dalam memperoleh gelar Sarjana Komputer di Universitas Pembangunan Nasional “VETERAN” Jatim.

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah membantu baik materiil maupun dorongan spirituil untuk menyelesaikan penulisan kerja praktek ini, terutama kepada:

1. Orang Tua dan kakakku tercinta serta kekasihku Febriani Mayaninggar atas motivasi dan doanya sehingga semua yang dikerjakan dapat berjalan lancar.
2. Bapak Prof. Dr. Ir. Teguh Soedarto, MP, selaku Rektor UPN “Veteran” Jatim.
3. Bapak Ir. Sutiyono, MT selaku DEKAN FTI UPN “VETERAN” Jatim.
4. Bapak Basuki Rahmat, S.Si., MT selaku Kepala Jur. Teknik Informatika, FTI UPN “VETERAN” Jatim dan selaku Dosen Pembimbing yang telah meluangkan waktu untuk memberikan bimbingan selama proses pelaksanaan Tugas Akhir penulis.
5. Bapak Achmad Junaidi, S.Kom, selaku Dosen Pembimbing yang telah meluangkan waktu untuk memberikan bimbingan selama proses pelaksanaan Tugas Akhir penulis.
6. Bapak Chrystia Aji P, S.Kom, selaku PIA TA yang telah mendukung proses pelaksanaan Tugas Akhir penulis.

7. Special to: Ardi Martono yang membantu dalam berpikir bersama dan laptop yang selalu setia membantu untuk mengerjakan ini semua.
8. Dosen-dosen Teknik Informatika dan Sistem Informasi, staff dan segenap civitas akademika UPN “VETERAN” Jatim.
9. My best Friends: Seluruh teman-teman yang sudah mendukung dan memberikan semangat dalam mengerjakan tugas akhir ini.

Penulis menyadari sepenuhnya masih banyak terdapat kekurangan dalam penulisan Tugas Akhir ini. Oleh sebab itu kritik serta saran yang membangun dari pembaca sangat membantu guna perbaikan dan pengembangan di masa yang akan datang.

Akhirnya dengan ridho Allah penulis berharap semoga Tugas Akhir ini dapat memberikan manfaat bagi pembaca sekalian terutama mahasiswa di bidang komputer.

Surabaya, 16 November 2011

Penulis

DAFTAR ISI

	Halaman
HALAMAN JUDUL	
LEMBAR PERSETUJUAN	
LEMBAR PENGESAHAN	
KETERANGAN REVISI	
MOTTO	
ABSTRAKSI	i
KATA PENGANTAR	ii
DAFTAR ISI	iv
DAFTAR TABEL	vii
DAFTAR GAMBAR	viii
DAFTAR ISTILAH	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah	3
1.3 Batasan Masalah	4
1.4 Tujuan	4
1.5 Manfaat Sistem Bagi Pengguna	5
1.6 Metodologi	5
BAB II LANDASAN TEORI	7
2.1 Sejarah Website dan Browser	7
2.2 Injeksi SQL	10
2.3 Injeksi XSS	15
2.4 Google Chrome	19
2.5 Membuat Add Ons Google Chrome	20
BAB III PERANCANGAN	24
3.1 Desain Sistem	24
3.2 Perancangan Sistem	26
3.3 Perancangan Data Input	27

3.4 Perancangan Proses	27
3.4.1 Proses Scanning	27
3.5 Perancangan Antar Muka	37
3.5.1 Blok Arsitektur Sistem WVS Online	37
3.5.3 Tampilan Antar Muka Aplikasi	39
3.5.4 Perancangan Uji Coba	39
BAB IV IMPLEMENTASI	42
4.1 Implementasi Sistem	42
4.1.1 Tampilan utama	42
4.1.2 Halaman Scanning SQL Injection pada URL	43
4.1.3 Halaman Scanning SQL Injection pada PAGE	45
4.1.4 Halaman Scanning SQL Injection pada SITE	47
4.1.5 Halaman Scanning XSS Injection pada URL	51
4.1.6 Halaman Scanning XSS Injection pada PAGE	53
4.1.7 Halaman Scanning XSS Injection pada SITE	56
4.1.8 Halaman Get Info about Domain Website	60
4.1.9 Halaman Get Info about Client Connection	62
4.1.10 Halaman Get Information about Cookie	64
4.1.11 Laporan Scanning Terakhir	66
BAB V PENGUJIAN DAN ANALISIS	68
5.1 Lingkungan Pengujian	68
5.2 Uji Coba	68
5.2.1 Aplikasi Web Vulnerability Scanner	68
5.2.2 Proses Scanning Secara Online	70
1) Scanning SQL Injection pada URL	72
2) Scanning SQL Injection pada PAGE	74
3) Scanning SQL Injection pada SITE secara cepat	77
4) Scanning SQL Injection pada SITE secara penuh	79
5) Scanning XSS Injection pada URL	82
6) Scanning XSS Injection pada PAGE	85

7) Scanning XSS Injection pada SITE secara cepat	88
8) Scanning XSS Injection pada SITE secara penuh	91
9) Get Info about Domain Website	94
10) Get Info about Client Connection	95
11) Get Information about Cookie	96
12) Laporan Scanning Terakhir	97
5.3 Analisis	99
BAB VI PENUTUP	103
6.1 Kesimpulan	103
6.2 Saran	104
DAFTAR PUSTAKA	

DAFTAR TABEL

	Halaman
Tabel 5.1 Daftar alamat website yang diperiksa	71
Tabel 5.2 Daftar 10 Website hasil scanning.....	100
Tabel 5.3 Daftar Website hasil scanning SQLI SITE (FULL).....	101
Tabel 5.4 Daftar Website hasil scanning XSS SITE (FULL).....	101

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Informasi yang valid dari website	14
Gambar 2.2 Informasi yang tidak valid dari website	14
Gambar 2.3 Informasi yang valid dari website	18
Gambar 2.4 Informasi yang tidak valid dari website	18
Gambar 2.5 Contoh extensi yang sudah jadi	20
Gambar 2.6 Pemasangan instalasi	22
Gambar 2.7 Hasil dari pemasangan extensi	23
Gambar 3.1 Perancangan Sistem Secara Global	25
Gambar 3.2 Diagram Alur Scan XSS	28
Gambar 3.3 Diagram Alur Scan terhadap URL	30
Gambar 3.4 Diagram Alur Scan pada PAGE	31
Gambar 3.5 Diagram Alur Scan pada SITE	33
Gambar 3.6 Diagram Alur Scan pada SITE Secara Cepat	34
Gambar 3.7 Diagram Alur Informasi Domain Website	35
Gambar 3.8 Diagram Alur Informasi Koneksi Pengguna	36
Gambar 3.9 Blok Arsitektur Sistem WVS.....	37
Gambar 3.10 Tampilan Antar Muka Aplikasi	38
Gambar 4.1 Tampilan Menu Utama	41
Gambar 4.2 Halaman Scanning SQL Injection pada URL	42
Gambar 4.3 Halaman Scanning SQL Injection pada PAGE	44
Gambar 4.4 Halaman Scanning SQL Injection pada SITE dengan cepat	47

Gambar 4.5	Halaman Scanning SQL Injection pada SITE secara penuh	48
Gambar 4.6	Halaman Scanning XSS Injection pada URL	52
Gambar 4.7	Halaman Scanning XSS Injection pada PAGE	54
Gambar 4.8	Halaman Scanning XSS Injection pada SITE dengan cepat	56
Gambar 4.9	Halaman Scanning XSS Injection pada SITE secara penuh	57
Gambar 4.10	Halaman Informasi Domain Website	60
Gambar 4.11	Halaman Informasi Client Connection	62
Gambar 4.12	Halaman Get Information about Cookie	64
Gambar 4.13	Halaman Pengunduhan result	66
Gambar 5.1	Tampilan Halaman Utama	69
Gambar 5.2	Tampilan sebelum diinjeksi SQL pada Tab Url	72
Gambar 5.3	Hasil Scanning SQL Injection pada Tab Url	73
Gambar 5.4	Tampilan sesudah diinjeksi SQL pada Tab Url	73
Gambar 5.5	Log scanning injeksi SQL pada Tab Url	74
Gambar 5.6	Tampilan sebelum diinjeksi SQL pada Page	75
Gambar 5.7	Hasil Scanning SQL Injection pada Page	75
Gambar 5.8	Tampilan sesudah diinjeksi SQL pada Page	76
Gambar 5.9	Log scanning injeksi SQL pada Page	76
Gambar 5.10	Tampilan sebelum diinjeksi SQL pada Site (cepat)	77
Gambar 5.11	Hasil Scanning SQL Injection pada Site (cepat)	78
Gambar 5.12	Tampilan sesudah diinjeksi SQL pada Site (cepat)	78
Gambar 5.13	Log scanning injeksi SQL pada Site (cepat)	79
Gambar 5.14	Tampilan sebelum diinjeksi SQL pada Site (penuh)	80
Gambar 5.15	Hasil Scanning SQL Injection pada Site (penuh)	80

Gambar 5.16	Tampilan sesudah diinjeksi SQL pada Site (penuh)	81
Gambar 5.17	Log scanning injeksi SQL pada Site (penuh)	81
Gambar 5.18	Tampilan sebelum diinjeksi XSS pada Tab Url	83
Gambar 5.19	Hasil Scanning XSS Injection pada Tab Url	83
Gambar 5.20	Tampilan sesudah diinjeksi XSS pada Tab Url	84
Gambar 5.21	Log scanning injeksi XSS pada Tab Url	84
Gambar 5.22	Tampilan sebelum diinjeksi XSS pada Page	85
Gambar 5.23	Hasil Scanning XSS Injection pada Page	86
Gambar 5.24	Tampilan sesudah diinjeksi XSS pada Page	87
Gambar 5.25	Log scanning injeksi XSS pada Page	87
Gambar 5.26	Tampilan sebelum diinjeksi XSS pada Site (cepat)	88
Gambar 5.27	Hasil Scanning XSS Injection pada Site (cepat)	89
Gambar 5.28	Pengisian script pada kotak search	89
Gambar 5.29	Tampilan sesudah diinjeksi XSS pada Site (cepat)	90
Gambar 5.30	Log scanning injeksi XSS pada Site (cepat)	90
Gambar 5.31	Tampilan sebelum diinjeksi XSS pada Site (penuh)	91
Gambar 5.32	Hasil Scanning XSS Injection pada Site (penuh)	92
Gambar 5.33	Tampilan sesudah diinjeksi XSS pada Site (penuh)	92
Gambar 5.34	Log scanning injeksi XSS pada Site (penuh)	93
Gambar 5.35	Informasi Domain Website	94
Gambar 5.36	Log Informasi Domain Website	94
Gambar 5.37	Informasi Client Connection	95
Gambar 5.38	Log Informasi Client Connection	95
Gambar 5.39	Hasil Get Information about Cookie	96

Gambar 5.40	Log Get Information about Cookie	96
Gambar 5.41	Pengunduhan result	97
Gambar 5.42	Hasil scanning Cookie dalam bentuk file dokumen.....	98
Gambar 5.43	Hasil scanning SQLI dalam bentuk file dokumen.....	98
Gambar 5.44	Penduplikasian alamat Url Hasil Scan SQLI.....	99
Gambar 5.45	Bukti hasil dari hasil scanning pada bentuk file simpan...	99

BAB I

PENDAHULUAN

1.1 Latar belakang

Internet pada era ini, sudah merebak di masyarakat. Banyak dari masyarakat sudah bisa menggunakan fasilitas-fasilitas yang ada di internet, seperti browsing dan download. Internet (kependekan dari interconnected-networking) ialah sistem global dari seluruh jaringan komputer yang saling terhubung menggunakan standar Internet Protocol Suite (TCP/IP) untuk melayani para pengguna di seluruh dunia. Banyak dari para pengguna internet belum memperhatikan dari segi keamanannya. Maka menjadi penting, untuk mengetahui bagaimana menjamin keamanan web. (Wibowo Tunardy: 2009).

Pengguna internet minimal harus mengetahui 3 konsep penting, seperti memastikan siapa relasi yang diajak untuk berkomunikasi di internet, menjaga kerahasiaan data-data, dan memastikan tidak ada komponen maupun data yang diakses mengalami kerusakan. Selain itu juga keamanan web berada di pihak masing-masing pengguna internet, karena apabila pengguna internet terlalu bebas dalam memberikan data-data penting, maka buka tidak mungkin, hacking akan mengambil informasi tersebut tanpa ijin.

Ada kemungkinan terjadinya hacking dikarenakan kesalahan dalam scripting pembuatan web yang dimanfaatkan oleh para hacker, sehingga rata-rata banyak website yang berhasil diserang melalui lubang ini. Kelemahan website yang ditemukan pada proses vulnerabilities scanner adalah XSS Injection dan SQL Injection yang akan dibahas dalam skripsi ini. Pengujian bisa dilakukan secara online dengan koneksi internet atau offline pada

komputer dengan memasang PHP, dan MySQL, atau memasang aplikasi seperti ataupun apache yang merupakan paket all in one.

Untuk dapat memakai internet memerlukan sebuah browser. Salah satu browser yang terkenal dan yang akan dipergunakan dalam skripsi ini adalah Google Chrome, merupakan browser buatan Google yang saat ini banyak digunakan oleh masyarakat dunia. Google melakukan beberapa perubahan pada setiap versi browser yang baru dirilis untuk memperbaiki kinerja dan kualitas browser Google Chrome. Bagi pengguna internet belum pernah mencoba aplikasi browser bernama Google Chrome ini, pada browser ini terdapat fitur-fitur yang sangat menarik dan bagus-bagus. Kemampuan Google Chrome tidaklah kalah dengan browser lainnya, seperti Firefox, Opera, dan Internet Explorer. Bahkan mungkin lebih baik.

Aplikasi Google Chrome versi terbaru saat ini, pengguna internet bisa menjumpai fitur Speed Dials, Private Browser, tab yang sangat dinamis, dan tentunya tampilan yang sederhana namun memukau. Google Chrome juga didukung oleh tema-tema yang menarik, seperti Firefox. Aplikasi Google Chrome mempunyai fitur Safe Browsing, dimana pengguna akan mendapatkan pemberitahuan jika ternyata pengguna mengunjungi sebuah situs yang berbahaya, seperti situs phishing atau situs yang mengandung malware.

Pada rilis terbaru saat ini, Google Chrome tidak hanya dapat digunakan dalam sistem operasi Windows saja, tetapi Google Chrome bisa juga digunakan untuk MacOS dan Linux.

Terdapat sebuah fitur tambahan yang bisa diintegrasikan dengan Google Chrome yang disebut Add Ons. Banyak Add Ons yang memiliki beberapa fitur yang membantu pengguna Google Chrome untuk menggunakan internet dengan lebih mudah. Dalam skripsi ini akan dirancang sebuah Add Ons yang memiliki fitur utama yaitu mendeteksi link yang dapat digunakan untuk XSS Injection dan SQL Injection.

Dari analisis di atas untuk mengatasi serangan pada sebuah web sehingga perlu dibuatnya sebuah aplikasi web yang menerapkan proses Vulnerabilities Scanner dengan serangan SQL (Structured Query Language) Injection dan XSS (Cross Site Scripting) Injection sehingga pengguna dapat mengetahui kelemahan yang terdapat pada sebuah web dalam bentuk sebuah Add Ons untuk browser dengan nama Google Chrome yang cukup terkenal.

1.2 Rumusan Masalah

Dari latar belakang yang telah dipaparkan oleh penulis sebelumnya maka penulis mencoba untuk membuat sebuah Add Ons pada browser Google Chrome dengan menerapkan proses Web Vulnerabilities Scanner. Adapun beberapa permasalahan yang ada sebagai berikut:

- a. Bagaimana membangun sebuah Add Ons untuk browser yang bernama Google Chrome yang menerapkan proses Web Vulnerabilities Scanner dan dengan serangan SQL (Structured Query Language) Injection dan XSS (Cross Site Scripting) berdasarkan alamat web yang diakses.

- b. Bagaimana membuat sebuah pola pendeteksian baik terhadap SQL (Structured Query Language) Injection dan XSS (Cross Site Scripting) pada alamat web yang diakses
- c. Bagaimana menampilkan dan menyimpan hasil proses Web Vulnerabilities Scanner untuk dapat dibaca oleh pengguna aplikasi tersebut.

1.3 Batasan Masalah

Dalam penyusunan tugas akhir ini, untuk mengatasi permasalahan yang ada maka penulis membatasi permasalahan sebagai berikut.

- a. Aplikasi ini dapat mendeteksi alamat Url pada website yang memungkinkan bisa dipergunakan sebagai media peretasan dengan XSS Injection dan SQL Injection.
- b. Aplikasi ini berkemampuan mendeteksi alamat Url pada website tersebut yang dituliskan pada halaman web dalam arti alamat tersebut tidak disembunyikan (enkripsi) dan dituliskan dalam tag HTML yaitu “HREF” dan sebuah “FORM” dalam tag html merupakan suatu kotak isian atau opsi dalam halaman web.
- c. Kecepatan proses Add Ons ini bergantung kecepatan internet yang terkoneksi pada komputer tersebut.

1.4 Tujuan Penelitian

Tujuan dari skripsi adalah bagaimana mengimplementasikan sebuah Web Vulnerability Scanner (WVS) dapat dibuat menjadi sebuah Add Ons

untuk browser Google Chrome. Serta sebagai syarat pelengkap untuk memenuhi Tugas Akhir di Universitas Pembangunan Nasional “veteran” Jatim.

1.5 Manfaat Penelitian

Adapun manfaat dibuatnya aplikasi Add Ons Web Vulnerability Scanner untuk browser Google Chrome ini adalah :

- a. Membantu pengguna internet untuk berhati hati saat memanfaatkan suatu website dalam hal keamanan informasi pada website tersebut.
- b. Membantu administrator mengetahui kelemahan apa saja yang ada pada website tersebut terhadap serangan SQL (Structured Query Language) Injection dan XSS (Cross Site Scripting).

1.6 Metode Penelitian

Beberapa metode yang dilaksanakan dalam penelitian ini adalah sebagai berikut :

a. Studi Literatur

Dilakukan dengan cara mencari segala macam informasi secara riset keperpustakaan dan mempelajari buku-buku yang berhubungan dengan masalah yang dihadapi.

b. Pengumpulan dan Analisa Data

Pengumpulan data dilakukan dengan cara : observasi, identifikasi dan klasifikasi melalui studi literatur. Dari pengumpulan data tersebut dapat

dilakukan analisa data yaitu dalam proses pembuatan Add Ons Web Vulnerability Scanner pada Google Chrome.

c. Perancangan Program

Melakukan analisa awal tentang Add Ons yang akan dibuat yaitu suatu pemecahan masalah yang dilakukan melalui system online dengan cara pembuatan Add Ons Web Vulnerability Scanner pada Google Chrome.

d. Pengujian dan Analisa

Pengujian dan analisa dimaksudkan untuk mengetahui sejauh mana sistem yang dibuat pada proyek akhir ini dapat berfungsi sesuai dengan proses sistem yang diharapkan.

e. Kesimpulan

Dibuat kesimpulan dari pengujian sistem tugas akhir dengan menguji apakah hasilnya seperti yang diharapkan pada tujuan tugas akhir sebelumnya.